

Appln No.: 10/071,820
Reply to Office Action of June 14, 2005

REMARKS/ARGUMENTS

CLAIMS 1-12

Claim 1

Claim 1 is:

A method for use with a postage meter system under the jurisdiction of a postal authority, the postage meter system comprising a host and a server, the host comprising a postal security device and postal indicia printing means, the server comprising a cryptographic device disposed for cryptographically secure communication with the postal security device, the method comprising the steps of:

entering information into the host indicative of a batch of mail pieces to be franked;

franking the mail pieces whilst storing information about the franking of the batch of mail pieces to a memory within the host;

within the postal security device, performing a cryptographic authenticating procedure upon the information about the franking of the batch and the information indicative of the batch, said information defining statistical information;

communicating the statistical information from the postal security device to the cryptographic device;

authenticating the statistical information at the cryptographic device; and

passing the statistical information to a postal authority.

In claim 1, the franking takes place *prior to* communication from the postal security device (which is within a host which also comprises a postal indicia printing means) to the cryptographic device (which is at a server). So far as the undersigned can discern, Cordery teaches away from this, teaching instead that various communications to and from some server occur *prior to* any franking by a postage meter.

Appln No.: 10/071,820
Reply to Office Action of June 14, 2005

The sequence of the steps cannot be ignored in considering this or any claim.

It is also noted that in the claim, it is the communication from the postal security device (which is within a host which also comprises a postal indicia printing means) *to the* cryptographic device (which is at a server), that is cryptographically authenticated. In contrast, so far as the undersigned can discern, in Cordery the only use of encryption is in connection with certain communications from the post office back to the mailer.

By teaching that the cryptographic communications be in the opposite direction from that set forth in the claim, Cordery appears to teach away in a second distinct way from the invention.

Finally, it will be appreciated that not all uses of cryptography are identical to each other. One use of cryptography, perhaps the use most familiar to lay persons, is encryption, which makes it difficult or impossible for an eavesdropper to learn the content of a message. A very different use of cryptography is authentication, which permits the receiver of a message to know that the sender is who it claims to be. This latter use is typically accomplished by cryptographic signing of a message or of a message digest or hash. These uses (encryption and authentication) are not at all the same thing.

Cordery, as best understood by the undersigned, speaks only of encryption uses. The claim, in contrast, speaks of authentication. As such, it appears that Cordery teaches away from the invention in this third distinct way.

For all these reasons it is requested that the rejection of claim 1 be reconsidered. Claims 2 through 12 should be allowed for the same reasons as claim 1.

Several additional arguments are provided below specifically for Claims 2-4, 6-8, and 11-12.

Appln No.: 10/071,820
Reply to Office Action of June 14, 2005

Claim 2

Claim 2 is:

The method of claim 1 wherein

the step of performing the cryptographic authenticating procedure comprises calculating a message authentication code, and

the step of authenticating the statistical information comprises checking for correctness of the message authentication code.

The undersigned has diligently studied the cited portion of Cordery (col. 2, line 10 to col. 3, line 30) and is unable to find message authentication codes anywhere in the cited portion, nor in the cited portion of Gilham. Reconsideration is requested.

Claim 3

Claim 3 is:

The method of claim 1 wherein

the step of performing the cryptographic authenticating procedure comprises digitally signing the statistical information, and

the step of authenticating the statistical information comprises checking for correctness of the digital signature.

The undersigned has diligently studied Cordery and is unable to find digital signing anywhere mentioned. The Examiner is requested to point out where this limitation can be found, or otherwise to withdraw the rejection of claim 3.

Claim 4

Claim 4 is:

Page 10 of 18

Appln No.: 10/071,820
Reply to Office Action of June 14, 2005

The method of claim 1 wherein the communicating step further comprises establishing a cryptographically secure session and communicating the information in a cryptographically secure fashion.

The undersigned has diligently studied Cordery and is unable to find this limitation anywhere mentioned. The Examiner is requested to point out where this limitation can be found, or otherwise to withdraw the rejection of claim 4.

Claim 6

Claim 6 is:

The method of claim 1 further comprising

the step of passing a confirmation from the cryptographic device to the postal security device indicative of receipt by the cryptographic device from the postal security device, and

the further step of deleting the statistical information from the postal security device upon receipt of the confirmation.

Nowhere in either of the cited references is the undersigned able to find either of these steps. Reconsideration is requested.

Claim 7

Claim 7 is:

The method of claim 1 further comprising the step, performed by the postal authority, of granting a discount based on the statistical information.

Nowhere in either of the cited references is the undersigned able to find anything remotely resembling this limitation. Reconsideration is requested.

Appln No.: 10/071,820
Reply to Office Action of June 14, 2005

Claim 8

Claim 8 is:

The method of claim 1 further comprising the step, performed by the postal authority, of granting a credit for future franking based on the statistical information.

Nowhere in either of the cited references is the undersigned able to find anything remotely resembling this limitation. Reconsideration is requested.

Claim 11

Claim 11 is:

The method of claim 1 where the step of communicating the statistical information from the postal security device to the cryptographic device further comprises the steps of:

cryptographically signing the statistical information within the postal security device, yielding a signature;

communicating the information and signature to memory within the host and not within the postal security device;

storing the information and signature within the memory within the host and not within the postal security device, and

communicating the information and signature from memory within the host and not within the postal security device, to the cryptographic device.

Nowhere in either of the cited references is the undersigned able to find anything remotely resembling these four limitations. The Examiner is requested to point out by page and line where in one or another of the references these four limitations may be found, or to withdraw the rejection of claim 11.

Appln No.: 10/071,820
Reply to Office Action of June 14, 2005

Claim 12

Claim 12 is:

The method of claim 11 wherein the storing of the information and signature within the memory within the host and not within the postal security device is for at least one day.

Nowhere in either of the cited references is the undersigned able to find anything remotely resembling this limitation. Reconsideration is requested.

CLAIMS 13-24

Claim 13

Claim 13 is:

A method for use with a postage meter system under the jurisdiction of a postal authority, the postage meter system comprising a host and a server, the host comprising a postal security device and postal indicia printing means, the server comprising a cryptographic device disposed for cryptographically secure communication with the postal security device, the host operated by a service provider providing service to a plurality of users, the method comprising the steps of:

entering information into the host indicative of a batch of mail pieces to be franked and indicative of an identity of a user associated with the batch;

franking the mail pieces whilst storing information about the franking of the batch of mail pieces to a memory within the host;

within the postal security device, performing a cryptographic authenticating procedure upon the information about the franking of the batch and the information indicative of the batch, said information defining statistical information;

communicating the statistical information from the postal security device to the cryptographic device;

Appln No.: 10/071,820
Reply to Office Action of June 14, 2005

authenticating the statistical information at the cryptographic device; and
passing the statistical information to a postal authority.

In claim 13, the franking takes place *prior to* communication from the postal security device (which is within a host which also comprises a postal indicia printing means) to the cryptographic device (which is at a server). So far as the undersigned can discern, Cordery teaches away from this, teaching instead that various communications to and from some server occur *prior to* any franking by a postage meter.

The sequence of the steps cannot be ignored in considering this or any claim.

It is also noted that in the claim, it is the communication from the postal security device (which is within a host which also comprises a postal indicia printing means) *to the* cryptographic device (which is at a server), that is cryptographically authenticated. In contrast, so far as the undersigned can discern, in Cordery the only use of encryption is in connection with certain communications from the post office back to the mailer.

By teaching that the cryptographic communications be in the opposite direction from that set forth in the claim, Cordery appears to teach away in a second distinct way from the invention.

Finally, it will be appreciated that not all uses of cryptography are identical to each other. One use of cryptography, perhaps the use most familiar to lay persons, is encryption, which makes it difficult or impossible for an eavesdropper to learn the content of a message. A very different use of cryptography is authentication, which permits the receiver of a message to know that the sender is who it claims to be. This latter use is typically accomplished by cryptographic signing of a message or of a message digest or hash. These uses (encryption and authentication) are not at all the same thing.

Appln No.: 10/071,820
Reply to Office Action of June 14, 2005

Cordery, as best understood by the undersigned, speaks only of encryption uses. The claim, in contrast, speaks of authentication. As such, it appears that Cordery teaches away from the invention in this third distinct way.

For all these reasons it is requested that the rejection of claim 13 be reconsidered. Claims 12 through 24 should be allowed for the same reasons as claim 13. Several additional arguments are provided below specifically for Claims 14-16, 18-20, and 23-24.

Claim 14

Claim 14 is:

The method of claim 13 wherein

the step of performing the cryptographic authenticating procedure comprises calculating a message authentication code, and

the step of authenticating the statistical information comprises checking for correctness of the message authentication code.

The undersigned has diligently studied the cited portion of Cordery (col. 2, line 10 to col. 3, line 30) and is unable to find message authentication codes anywhere in the cited portion, nor in the cited portion of Gilham. Reconsideration is requested.

Claim 15

Claim 15 is:

The method of claim 13 wherein

the step of performing the cryptographic authenticating procedure comprises digitally signing the statistical information, and

Appln No.: 10/071,820
Reply to Office Action of June 14, 2005

the step of authenticating the statistical information comprises checking for correctness of the digital signature.

The undersigned has diligently studied Cordery and is unable to find digital signing anywhere mentioned. The Examiner is requested to point out where this limitation can be found, or otherwise to withdraw the rejection of claim 15.

Claim 16

Claim 16 is:

The method of claim 13 wherein the communicating step further comprises establishing a cryptographically secure session and communicating the information in a cryptographically secure fashion.

The undersigned has diligently studied Cordery and is unable to find this limitation anywhere mentioned. The Examiner is requested to point out where this limitation can be found, or otherwise to withdraw the rejection of claim 16.

Claim 18

Claim 18 is:

The method of claim 13 further comprising

the step of passing a confirmation from the cryptographic device to the postal security device indicative of receipt by the cryptographic device from the postal security device, and

the further step of deleting the statistical information from the postal security device upon receipt of the confirmation.

Nowhere in either of the cited references is the undersigned able to find either of these steps. Reconsideration is requested.

Appln No.: 10/071,820
Reply to Office Action of June 14, 2005

Claim 19

Claim 19 is:

The method of claim 13 further comprising the step, performed by the postal authority, of granting a discount to the user associated with the batch based on the statistical information.

Nowhere in either of the cited references is the undersigned able to find anything remotely resembling this limitation. Reconsideration is requested.

Claim 20

Claim 20 is:

The method of claim 13 further comprising the step, performed by the postal authority, of granting a credit for future franking to the user associated with the batch based on the statistical information.

Nowhere in either of the cited references is the undersigned able to find anything remotely resembling this limitation. Reconsideration is requested.

Claim 23

Claim 23 is:

The method of claim 13 where the step of communicating the statistical information from the postal security device to the cryptographic device further comprises the steps of:

cryptographically signing the statistical information within the postal security device, yielding a signature;

communicating the information and signature to memory within the host and not within the postal security device;

storing the information and signature within the memory within the host and not

Appln No.: 10/071,820
Reply to Office Action of June 14, 2005

within the postal security device, and

communicating the information and signature from memory within the host and not within the postal security device, to the cryptographic device.

Nowhere in either of the cited references is the undersigned able to find anything remotely resembling these four limitations. The Examiner is requested to point out by page and line where in one or another of the references these four limitations may be found, or to withdraw the rejection of claim 23.

Claim 24

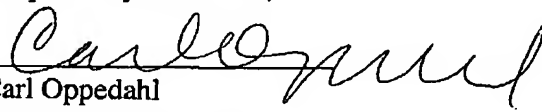
Claim 24 is:

The method of claim 23 wherein the storing of the information and signature within the memory within the host and not within the postal security device is for at least one day.

Nowhere in either of the cited references is the undersigned able to find anything remotely resembling this limitation. Reconsideration is requested.

For these reasons, this application is now considered to be in condition for allowance and such action is earnestly solicited.

Respectfully submitted,


Carl Oppedahl
PTO Reg. No. 32,746
Oppedahl & Larson LLP
P O Box 5068
Dillon, CO 80435-5068
970-468-6600